Volume 4, Issue 12, December 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Detection and Prevention of Misleading Routing Attack in Mobile Ad-hoc Networks

Ritu, Seema Sabharwal (Assistant Professor)
GIMT, Kanipla, Kurukshetra,
Haryana, India

Abstract— Wireless networks are gaining popularity to its peak in these days, as the users want wireless connectivity irrespective of their geographic location. Due to popularity of MANET, there is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. The node presents itself in such a way to the node that it can attack other nodes and networks knowing that it has the shortest path. Mobile Ad-hoc Network must have a secure way for transmission and communication which is quite difficult and very important issue. The scope of this paper is to study the effects of Black hole attack in MANET Ad-Hoc On Demand Distance Vector (AODV) Routing protocol and detect the attack with securing the communication.

Keywords— MANET, RREQ, MIRA

I. INTRODUCTION

Mobile Ad-Hoc Networks are autonomous and decentralized wireless network. MANETs have mobile nodes that are free in moving in anywhere of the network. Mobile nodes may be mobile phone, laptop, MP3 player and personal computer that are participating in the network and are mobile. Security in MANET is the most important issue for the proper working of the network. The availability, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs regularly suffer from security attacks for the reason that of its features like open medium, lack of central monitoring and management, supportive algorithms and no clear defense mechanism.

There are currently three main routing protocols for ad hoc networks [1], Destination-Sequenced Distance Vector routing (DSDV) [5], Dynamic Source Routing (DSR) [4], and AODV [2]. DSDV is a table driven routing protocol. Each mobile node in the network maintains a routing table with entries for every possible destination node. The routing table is from time to time updated for every change in the network to maintain consistency. This involves regular route update broadcasts. DSR is an on-demand routing protocol and it maintains a route cache, which consume lot of memory. AODV is an on-demand routing protocol. Each mobile node maintains a routing table that contains the next hop information for a route to the destination . When a source node wants to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table. If route not available, it starts a route discovery process by sending the Route Request (RREQ) message to its neighbors, which is further propagated until it reaches destination by intermediate node.

The AODV protocol is vulnerable to the well-known black hole attack. This black hole is a mobile node that always responds positively with a RREP message to every RREQ, even though it does not really have a valid route to the destination node. While a black hole does not have to check its routing table, it is the first to respond to the RREQ in most cases. If the data packets routed by the source node reaches the black hole node, it drops the packets rather than forwarding them to the destination node. Deng, Li, and Agrawal [3] assume the black hole nodes do not work as a group and propose a solution to identify a single black hole. There are many type of attack that affect the performance of the MANET. In this paper, we are proposed a solution of the Downstream Attack which is a kind of Black hole attack stated by F. Kandah et. al. [6].

II. RELATED WORK

An The attacks can be categorized on the basis of the source of the attacks i.e. Internal or External, and on the behavior of the attack i.e. Passive or Active attack. This classification is important because the attacker can exploit the network either as internal, external or/ as well as active or passive attack against the network.

External attackers are mainly outside the networks who want to get access to the network and once they get access to the network they start sending bogus packets, denial of service in order to disrupt the performance of the whole network. While in internal attack the attacker wants to have normal access to the network as well as participate in the normal activities of the network. The attacker gain access in the network as new node either by compromising a current node in the network or by malicious impersonation and start its malicious behavior. Internal attack is more severe attacks then external attacks.

In active attack the attacker disrupts the performance of the network, steal important information and try to destroy the data during the exchange in the network [7]. In Passive attack, the attacker listen to network in order to get information, what is going on in the network[7]. It listens to the network in order to know and understand how the nodes are communicating with each other, how they are located in the network. Before the attacker launch an attack to the network, the attacker has all related information about the network that it can easily take control and introduce attack in the network.

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This malicious node advertises its availability of fresh routes irrespective of checking its routing table. Such a way attacker node will always have the availability in replying to the route request and thus interrupt the data packet and keep it [8].When source flood the RREQ packet, malicious node reply will be received by the requesting node before the reception of reply from actual node, hence a malicious and forged route is created. When this malicious route is created, now it is depend upon the malicious node whether to drop all the packets or forward it to the unknown address [9].

Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack. Internal black hole attack has an internal malicious node which fits in between the routes of given source and destination. It gets the chance this malicious node make itself an active data route element. Now it is capable of conducting attack with the start of data transmission. Such type of attack is an internal attack because node itself belongs to the data route. This type of attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node. External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. This type of attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET.

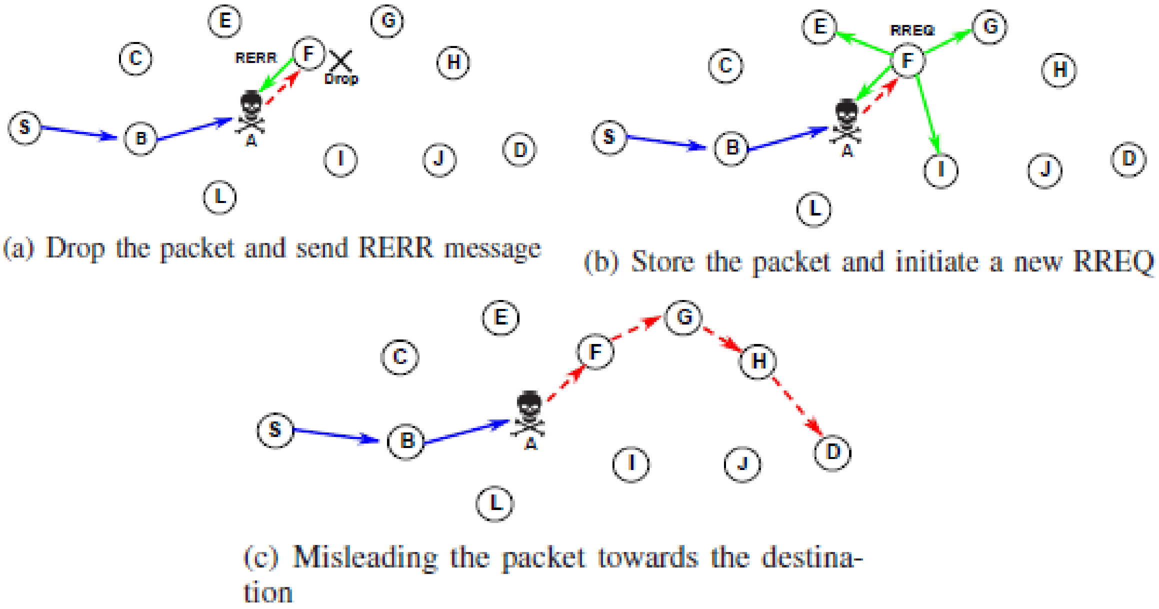
Gray Hole [10] attacker misleads the network by agreeing to forward the packets in the network. It receive the packets from the neighboring node, the attacker drop the packets. In the beginning the attacker nodes behaves normally and reply true RREP messages to the nodes that started RREQ messages. When it receives the packets it starts dropping the packets and launch Denial of Service (DoS) attack.

The flooding attack is easy to implement but cause the most damage. Flooding attack can be achieved either by using RREQ or Data flooding [11]. In RREQ flooding the attacker floods the RREQ in the whole network which takes a lot of the network resources. This task can be done by the attacker node by selecting such I.P addresses that do not exist in the network. By doing this, any node is not able to answer RREP packets to these flooded RREQ.

In MANETs the nodes perform collaboratively in order to forward packets from one node to another node. When a node decline to work in partnership to forward packets in order to save its limited resources are termed as selfish node, such type of condition cause mainly network and traffic disruption [11]. The selfish nodes can refuse by advertising non existing routes among its neighbor nodes or less optimal routes.

The nature of Ad-Hoc network is that any node can join freely the network and can leave it. Nodes which want to attack on the network join the network. The malicious node then afterward exploits the irregularities in the network surrounded by the nodes. It involved in the transmission and later on some stage launches the message modification attack [7].

Downstream misleading attack [6], source node will keep sending to its next hop indicated in its routing table, until a further update (receiving an RERR message). Let us assume that the delay from the source to the adversary is fixed. In order for the adversary to delay the packets relayed to the destination node, it will use the information collected from the RREP message that it received from the destination. The adversary knows which of his next hop has the best path to the destination, so in order to mislead the packet, it will relay the packet to any other neighbor not the one specified by the routing protocol. This type of attack (downstream misleading attack) will increase the delay from S to D.



(a) Drop the packet and send RERR message

(b) Store the packet and initiate a new RREQ

(c) Misleading the packet towards the destination

The blue arrows show the path traced by the packet on a route attracted by the adversary A, while red colored dashed arrows depict the path on which the packet is forwarded after being misled by A. The green arrows show the new RREQ/RRER messages initiated by node F on receipt of an unexpected packet. When the adversary receives a packet, it will try to delay the packet by relaying it to a different route using a node which was not specified by the routing information. Compared to the normal path from source S to destination D (S-B-A-I-J-D), the adversary A will relay the packet(s) to node F, instead of node I to mislead the packet.

Three situations could occur. First, in Fig. a, node F will look into its routing table for a recent route to the destination. If there is no active route for this request, node F will drop the packet and send an RERR message back to the source indicating that a path does not exist. The second situation is shown in Fig. (b), node F, without any active path for the request, will choose to store the packet in its queue and generate a new RREQ to find a path to the destination. In this case, the adversary A can again capture the RREQ from node F, and send back some forged information about having the best route to the destination. If node F realizes that node A has a path, it could suspect that node A is sending some forged information of the path. But F cannot guarantee that A is malicious due to mobility. It is possible that a new path has emerged in A's neighborhood. In the third scenario shown in Fig. c, node F finds a recent route to the destination which is not expired. In this case, it will stick with the information in its routing table and send the packet to the next hop specified in the routing table. It is worth noting that more time will be consumed by the sender in waiting for an ACK in all the situations.

III. Proposed Work

Proposed method is a delay based attack detection technique which uses Round Trip Time (RTT) and Smooth Round Trip Time. In this technique we continuously monitor the RTT and SRTT when packet acknowledgement comes to the source. When an acknowledgment receives from the destination, source calculates RTT and update the SRTT accordingly. If difference of RTT and SRTT is greater than threshold then sender stop sending the data packet and search for new path from source to destination. Procedure of the proposed technique is given as follows:

- When source S receive RREP from destination D then it store it as a smooth round trip time.
- Now sender send data packet to destination and wait for ACK. When ACK receive by the sender then it calculate round trip time (RTT).
- After calculation of RTT, we calculate difference of current round trip time and smooth round trip time by using following equations

$$SRTT = \alpha SRTT + (1 - \alpha)RTT$$

$$D = \beta(RTT - SRTT)$$

Where α is a smoothing factor equals to 0.825 and $\beta=3/4$.

- If D>threshold then source stop sending the data packet and try to change the path from the source to destination.
- Threshold is calculated according to SRTT value by using following equation

$$Th = 5 * SRTT$$

means if D is greater than 5 times of SRTT then source stop sending data packet

IV. Simulation Result

This experiment result was carried out using NS-2. The following subsection provides details of the simulation environment, metrics and experimental results. Ns-2 is an open source discrete event simulator used by the research community for research in networking. It has support for both wired and wireless networks and can simulate several network protocols such as TCP, UDP, multicast routing, etc. More recently, support has been added for simulation of large satellite and ad hoc wireless networks.

Simulation Environment

- **Grid Size:** 1000x1000 Meters
- **Number of Nodes:** 40 nodes
- **Routing Protocol:** AODV was used.
- **Mobility:** Random waypoint model was used with maximum speed set to 20 meters per second. Pause time was set to 15 seconds
- **Packet Traffic:** 2 TCP connections and 2 UDP connection

Figure 3 shows that the proposed scheme provides better result in terms of packet delivery ratio with number of nodes. In this graph, we run our simulation by changing the number of node in between 20 to 40 and calculate the result. Basic AODV provide higher result shown in graph but when apply black hole attack then MRIA graph shows the performance is very low in comparison with AODV. When we simulate our proposed protocol then we get better result than MIRA.

In next simulation, we compare the performance of our proposed method with AODV and MIRA. Figure 4 shows that our proposed protocol provides better result than MIRA.

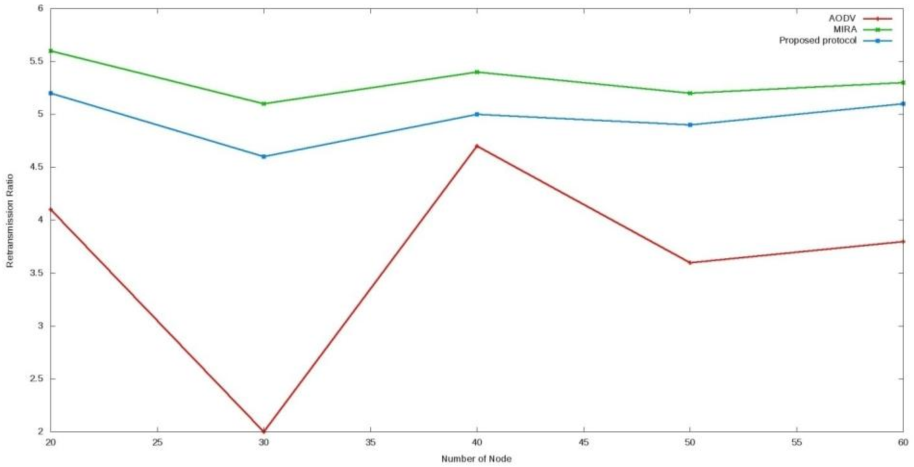


Figure 4

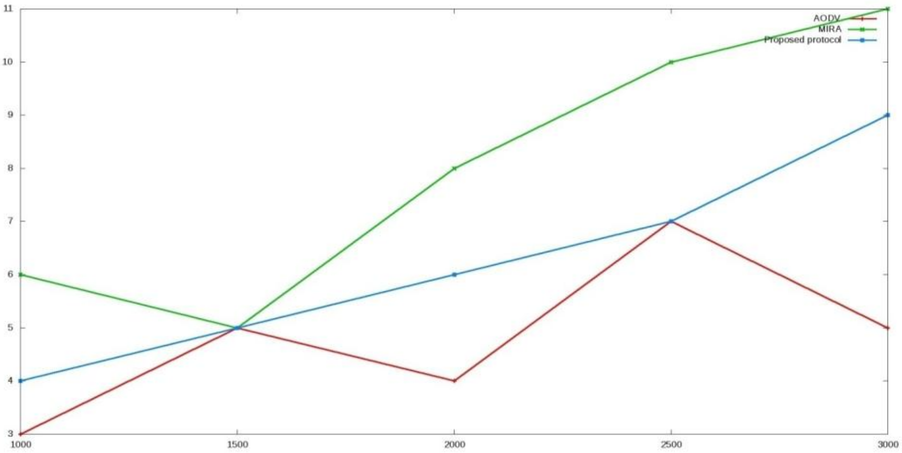


Figure 5

Figure 5 shows that the proposed method provides better result than MIRA in terms of packet retransmission. We simulate our proposed protocol with MIRA and basic AODV and compare it. Our proposed method reduces the number of retransmitting packet than MIRE protocols

V. Conclusion

In this study, we analyzed effect of the Black Hole in an AODV Network. For this purpose, we implemented an AODV protocol that behaves as Black Hole in NS-2. We simulated five scenarios where each one have 20 to 40 nodes that use AODV protocol and also simulated the same scenarios after introducing one Black Hole Node into the network. Having simulated the Black Hole Attack, we saw that the packet loss is increased in the ad-hoc network.

We proposed a new technique that uses acknowledgement delay to detect the black hole attack and avoid the path for next packet transmission. Simulation result shows that our proposed method reduces the retransmission and increase the packet delivery ratio. Due to delay analysis our proposed method reduce packer drop ratio which increase the performance of TCP and increase packet delivery ratio.

VI. FUTURE SCOPE

In this paper we proposed a delay base Black Hole detection and prevention technique. Future scope of this work is to improve the proposed method based on different parameters like packet delivery notification, sequence number monitoring and other factor related to black hole attack.

References

[1] Elizabeth M. Royer, and Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," IEEE Personal Communications, pp. 46-55, April 1999.

[2] Charles E. Perkins, and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector (AODV) Routing," Internet Draft, November 2002.

[3] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magzine, vol. 40, no. 10, October 2002.

[4] David B. Johnson, and David A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," *Mobile Computing*, edited by Tomasz Imielinski and Hank Korth, Chapter 5, pages 153-181, Kluwer Academic Publishers, 1996.

[5] C. E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,” Computer Communications Review, pp. 234-244, October 1994.

[6] F. Kandah, Y. Singh, W.Zhang_, T. Wang," Misleading Routing Attack in Mobile Ad-hoc Networks"IEEE Globecom 2011 proceedings.

[7] C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, “A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks,” Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.

[8] K. Biswas and Md. Liaqat Ali, “Security threats in Mobile Ad-Hoc Network”, Master Thesis, Blekinge Institute of Technology” Sweden, 22nd March 2007.

[9] G. A. Pegueno and J. R. Rivera, “Extension to MAC 802.11 for performance Improvement in MANET”, Karlstads University, Sweden, December 2006

[10] S.Marti, T.J.Giuli, K.Lai, M.Baker, “Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks”.

[11] M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, “A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks,” Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.